Designing for Accountability: A Checklist for Accountable Information Systems

Lalana Kagal
Decentralized Information Group
MIT Computer Science & Artificial Intelligence Lab
Our Accountability Approach to Privacy

- When security approaches (access control, anonymization, etc.) are insufficient for privacy
  - Re-identification of medical records (Sweeney)
  - Facebook friends expose sexual orientation (Jernigan and Mistree)
  - Breaking anonymity of the Netflix prize dataset (Narayanan and Shmatikov)

- Accountability
  - Supplementary (and not replacement) approach to upfront prevention
  - Enables users to be compliant with applicable policies/laws
  - Threat model: non-malicious users
Our Accountability Approach to Privacy

- When information has been **used**, it should be possible to determine what happened, and to pinpoint use that is inappropriate.

- Move focus from “what you know” about me to “what you do with it”

- Not just access control but **usage control**

Graphic courtesy Ilaria Liccardi
Essential Aspects of Accountable Systems

**Capability 1: Policy compliance**

- Should be possible to verify that a certain data request, transfer or use is compliant under applicable policies
  - **Requirement:** Machine-understandable policies & policy reasoner
  - **Requirement:** Machine-understandable user preferences
  - **Requirement:** Human readable justifications for policy decisions
  - **Requirement:** View of data collected by system
Example: Machine-understandable Policy Language

- AIR is a machine-readable rule/policy language
- based on Linked Data technologies
- focussed on justification generation, ease of specification, rule reuse, and builtins for use of distributed data
- Has been used in various projects for information accountability, policy compliance, trust frameworks, access control, etc.

```prolog
@forAll :PERSON, :CITY.
:ny_state_residency_policy a air:Policy;
    air:rule :state-residency-rule.

:state-residency-rule a air:Belief-rule;
    rdfs:label "state residency rule";
    air:if {
        :PERSON tamip:Lives_in_city :CITY.
        :CITY tamip:Has_state :NY.
    };
    air:then{air:description{"lives in the NY state city -" :CITY};
    air:assert {"PERSON air:compliant-with :ny_state_residency_policy."}].
```

AIR rule that checks state residency
Example: Policy compliance checker

Information Sharing Between
Government Agencies
Example: Policy compliance justification

<table>
<thead>
<tr>
<th>Issue:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whether the transactions comply with Massachusetts General Law, Part I, Title II, Chapter 6, Section 172</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule(s) is/are specified in the policy file</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Analysis:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Request for Information about Robert B. Guy is a dissemination by Mia Analysis to Fred Agent, designated as Transaction.</td>
</tr>
<tr>
<td>- Request for Information about Robert B. Guy contains Criminal Offender Record Information, and Fred Agent is a member of a Criminal Justice Agency as required by MGL 6-172, Para. 1, Sent. 1a.</td>
</tr>
<tr>
<td>- Compliance additionally requires: Fred Agent is performing Criminal Justice Duties and Request for Information about Robert B. Guy limited to data necessary for Fred Agent’s Criminal Justice Duties, as required by MGL 6-172, Para. 1, Sent. 2, Cl. 1.</td>
</tr>
<tr>
<td>- Compliance additionally requires that Fred Agent is certified by the board as qualified for access, as required by MGL 6-172 Paragraph 2.</td>
</tr>
<tr>
<td>- Compliance additionally requires: The agency to which Mia Analysis belongs shall maintain, for such period as the board shall determine, a listing of the agencies or individuals to which it has released or communicated such information, as required by MGL 6-172, Para. 4, Sent. 1.</td>
</tr>
<tr>
<td>- Inquiry is about Robert B. Guy and is based on a personally identifying characteristic, as required by MGL 6-172 Para. 5, Sent. 1, Cl. 2.</td>
</tr>
<tr>
<td>- Fred Agent performs function investigation.</td>
</tr>
<tr>
<td>- Compliance additionally requires that release of Request for Information about Robert B. Guy would not violate any other provisions of state or federal law, as required by MGL 6-172, Para. 6, Sent. 1(b), Cl. 3.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conclusion:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The transaction - Transactions is compliant with Massachusetts General Law, Part I, Title II, Chapter 6, Section 172</td>
</tr>
</tbody>
</table>
Example: Policy compliance enabler

Enabling Creative Common License Compliance
Example: View of data collected by system

W3C Privacy Dashboard
Essential Aspects of Accountable Systems

• Capability 2: Provenance management
  - Provenance of information such as its source, creator, etc. should be maintained
  - Requirement: Tracking information as it flows through the systems and machine understandable provenance annotations
  - Requirement: Define how information has produced/combined/generated from different sources
Example: Provenance ontology

W3C Provenance (PROV) Ontology

- type=foaf:Organization, prov:Agent
  - :government
    - prov:wasAttributedTo
      - :crimeData
    - prov:used
      - :aggregationActivity
        - prov:startedAtTime: "2011-07-14T01:01:01Z"^^xsd:dateTime
        - prov:endedAtTime: "2011-07-14T02:02:02Z"^^xsd:dateTime
  - :civil_action_group
    - prov:wasAttributedTo
      - :nationalRegionsList
    - prov:used
      - :aggregationActivity
        - prov:startedAtTime: "2011-07-14T01:01:01Z"^^xsd:dateTime
        - prov:endedAtTime: "2011-07-14T02:02:02Z"^^xsd:dateTime

- type=foaf:Organization, prov:Agent
  - foaf:name="National Newspaper Inc."
  - :national_newspaper_inc
    - prov:actedOnBehalfOf
      - :derek
        - prov:givenName="Derek"
        - foaf:mbox=<mailto:derrek@example.org>
      - :national_regions_list
        - prov:wasAttributedTo
          - :aggregated_by_regions
            - prov:wasGeneratedBy
              - :illustration_activity
                - prov:wasGeneratedBy
                  - :bar_chart
Example: Provenance tracking

Provenance Enabled Client

Verification Service

WebID Access Delegation

Data Transfer

Verified Identity

Web Server

Provenance Logs

Provenance Tracker Network

Transparent Health: Decentralized Tracking of Electronic Health Records
Essential Aspects of Accountable Systems

- Capability 3: Violation detection and identification
  - When information is **misused**, it should possible be to identify the violation and the violator
  - Requirement: Tracking all uses of data and ability to identify users (accountable anonymity *)
  - Requirement: Machine-understandable policies & policy reasoner
  - Requirement: Machine-understandable user preferences
Example: Violation verification

Accountability at the HTTP level
Essential Aspects of Accountable Systems

- Capability 4: Audit of system
  - Study how a system **collects and uses** private information
  - Requirement: Extensive audit logs of data requests, transfers, and all uses
  - Requirement: Machine-understandable policies & policy reasoner or auditing mechanism
Example: Privacy audit

The user may not query specifically for people living in New England

The user is filtering on city with value set to Boston, which is in New England

Query 1 contains lives-in attribute city with value Boston

Auditing Queries to Sensitive Database Systems
Example: Privacy audit

Audit Logs for conditions

Date: 12 Sep 2013  
Agent: Doctor Dee  
Role: Physician  
Purpose: Preparation for a follow up visit

Date: 23 Sep 2013  
Agent: Steven Special  
Role: Physician  
Purpose: Referral Visit

Date: 23 Sep 2013  
Agent: Pocilia Philip  
Role: Pharmacist  
Purpose: Check Prescription History

Transparent Health: Decentralized Tracking of Electronic Health Records
Essential Aspects of Accountable Systems

- Capability 5: Policy awareness
  - Provide understandable view of policy to users to encourage appropriate behavior
  - Requirement: Users manipulate information via policy-aware interfaces that signal compliant / non-compliant uses
Example: Policy-aware Interfaces

Policy Awareness Application in Facebook

Policy Awareness in Linked Data Browser
Example: Policy-aware Interfaces

Creative Common License Awareness
Essential Aspects of Accountable Systems

- Capability 6: Redress mechanism
  - When information is misused, it should possible be to identify the violation and the violator and take action
Example: Redress mechanisms

- Email address to send complaints/grievances
  - Google dashboard
- Reputation and trust frameworks
  - ebay, BBB, amazon
- Legal
  - take down notice, cease and desist
- Other?
Challenges for Accountable Information Systems

- not a pure technical solution
  - technology + social + regulation

- technical challenges
  - tracking data across different systems, at different levels
  - tracking data that has been significantly transformed
  - provenance information itself can be sensitive and needs to be protected
  - generating machine understandable policy
  - (semi) automatically identifying the purpose of the data use and subsequent misuse
  - efficient techniques that provide policy compliance, violation identification, and auditing

- social
  - how to incentivize accountability
  - effective redress mechanisms
  - educating users/system administrators
Thank you

- http://dig.csail.mit.edu